Discrete Mathematics 43 (1983) 65–78
North-Holland Publishing Company



# NON-SKEW SYMMETRIC ORTHOGONAL MATRICES WITH CONSTANT DIAGONALS

Clement W. H. LAM*

*Department of Computer Science, Concordia University, Montreal, Canada*

Received 17 September 1981
Revised 16 February 1982

A matrix $C$ of order $n$ is orthogonal if $CC^T = dI$. In this paper, we restrict the study to orthogonal matrices with a constant $m > 1$ on the diagonal and $\pm 1$'s off the diagonal. It is observed that all skew symmetric orthogonal matrices of this type are constructed from skew symmetric Hadamard matrices and vice versa. Some simple necessary conditions for the existence of non-skew orthogonal matrices are derived. Two basic construction techniques for non-skew orthogonal matrices are given. Several families of non-skew orthogonal matrices are constructed by applying the basic techniques to well-known combinatorial objects like balanced incomplete block designs. It is also shown that if $m$ is even and $n \equiv 0 \pmod 4$, then an orthogonal matrix must be skew symmetric. The structure of a non-skew orthogonal matrix in the special case of $m$ odd, $n \equiv 2 \pmod 4$ and $m \geq \frac{1}{6}n$ is also studied in detail. Finally, a list of cases with $n \leq 50$ is given where the existence of non-skew orthogonal matrices are unknown.

## 1. Introduction

A matrix $C$ is *orthogonal* if $CC^T = dI$ where $d$ is a constant and $I$ is the identity matrix. In this paper, we are interested in studying orthogonal matrices of order $n$ with constant integral diagonal $m > 1$ and off diagonal entries $\pm 1$. Thus, they satisfy

$$CC^T = (m^2 + n - 1)I. \tag{1.1}$$

Such a matrix $C$ is called a *solution* to (1.1). A matrix $C$ is *skew symmetric* or simply *skew*, if $C_{ij} = -C_{ji}$ for $i \neq j$.

Solutions to (1.1) were studied in [6], which was mainly interested in the case where $C$ is symmetric. In this paper, we are interested in the more general situation where $C$ need not be symmetric. We show first that skew symmetric solutions to (1.1) are all constructed from skew symmetric Hadamard matrices and are thus less interesting. In Section 2, the basic properties of solutions to (1.1) are presented. We also derive some simple necessary conditions for the existence of non-skew symmetric solutions. In Section 3, several constructions of non-skew symmetric solutions are presented. Section 4 studies the special case where $n \equiv 0 \pmod 4$ and $m$ is even and shows that all such solutions are skew symmetric.

* This paper was written while the author was visiting the Applied Mathematics Department of the University of Sydney.

Section 5 studies the special case where $n \equiv 2 \pmod 4$ and $m \geq \frac{1}{6}n$. It gives a canonical form for a non-skew symmetric solution as well as various necessary conditions. Section 6 presents a table of parameters with $n \leq 50$ where the existence of a non-skew solution is unknown.

In the constructions presented in Section 3, we use the standard combinatorial objects like a symmetric balanced incomplete block design or SBIBD, a Hadamard matrix, a difference set and an orthogonal design. The reader is referred to the standard references [1, 4, 5].

## 2. Basic properties

In [6], it was noted that if $H$ is a skew-symmetric Hadamard matrix, then $C=(m-1)I+H$ is a skew-symmetric solution for every integer $m$. Conversely, it is simple to show that if $C$ is a skew solution, then $H=C-(m-1)I$ is skew Hadamard. Thus, skew solutions to (1.1) are less interesting in our context and the rest of the paper is concerned with non-skew solutions.

The property that $C$ is a solution is preserved by any combination of simultaneous row and column permutation, simultaneous changing of signs in a whole row and column, or taking the transpose. Two solutions are *equivalent* if one can be changed to the other by using a combination of the above operations.

By changing the signs of appropriate columns, the first 3 rows can be put in the form of Fig. 2.1, where $x_1, \dots, x_6$ can be either $+1$ or $-1$.

$$\begin{array}{lccccccc}
\text{Row 1:} & m & x_1 & x_2 & 1\cdots 1 & 1\cdots 1 & 1\cdots 1 & 1\cdots 1 \\
\text{Row 2:} & x_3 & m & x_4 & 1\cdots 1 & 1\cdots 1 & -\cdots- & -\cdots- \\
\text{Row 3:} & x_5 & x_6 & m & \underbrace{1\cdots 1}_{a} & \underbrace{-\cdots-}_{b} & \underbrace{1\cdots 1}_{c} & \underbrace{-\cdots-}_{d}
\end{array}$$

Fig. 2.1.

The entries $x_1$ and $x_2$ can also be forced to be $+1$'s. However, they are left as variables for future use.

Considering the number of columns and inner product of these 3 rows, we get

$$3+a+b+c+d=n, \tag{2.1}$$

$$m(x_1+x_3)+x_2x_4+a+b-c-d=0, \tag{2.2}$$

$$m(x_2+x_5)+x_1x_6+a-b+c-d=0, \tag{2.3}$$

$$m(x_4+x_6)+x_3x_5+a-b-c+d=0. \tag{2.4}$$

Solving for $a, b, c$ and $d$ in terms of $x_1, \dots, x_6$, $n$ and $m$, we get

$$4a=n-m(x_1+x_2+x_3+x_4+x_5+x_6)-x_1x_6-x_2x_4-x_3x_5-3, \tag{2.5}$$

$$4b=n-m(x_1-x_2+x_3-x_4-x_5-x_6)+x_1x_6-x_2x_4+x_3x_5-3, \tag{2.6}$$

$$4c=n-m(-x_1+x_2-x_3-x_4+x_5-x_6)-x_1x_6+x_2x_4+x_3x_5-3, \tag{2.7}$$

$$4d=n-m(-x_1-x_2-x_3+x_4-x_5+x_6)+x_1x_6+x_2x_4-x_3x_5-3. \tag{2.8}$$

**Proposition 2.1.** *If $m \geq \frac{1}{2}n$, then a solution to* (1.1) *is skew symmetric.*

**Proof.** Suppose a solution $C$ exists which is non-skew. Then there exists a pair of indices $i$ and $j$ such that $C_{ij} = C_{ji}$. Permute these entries such that they correspond to $x_1$ and $x_3$ of Fig. 2.1 and also force $x_1 = x_3 = +1$. Adding (2.1) and (2.2), we get

$$2m+3+x_2x_4+2(a+b) = n.$$

Since $a+b \geq 0$ and $x_2x_4 \geq -1$, we have $2m \leq n-2$ which contradicts $m \geq \frac{1}{2}n$. □

**Proposition 2.2.** *The order $n$ is even.*

**Proof.** We add (2.1) to (2.2) and observe that both $x_1+x_3$ and $3+x_2x_4$ are congruent to 0 modulo 2. □

**Proposition 2.3.** *If $C$ is non-skew and $m$ is odd, then $n \equiv 0 \pmod 4$.*

**Proof.** Without loss of generality, we assume that the first 3 rows are of the form in Fig. 2.1 with $x_1 = x_2 = x_3 = +1$. Then (2.5) becomes

$$(3+x_4+x_5+x_6)(m+1)+4a = n.$$

Since $3+x_4+x_5+x_6 \equiv 0 \pmod 2$ and $m$ is odd, we have $n \equiv 0 \pmod 4$. □

In Section 4, we will prove the analogous result that if $C$ is non-skew and $m$ is even, then $n \equiv 2 \pmod 4$.

By using a result of Raghavarao, van Lint and Seidel [4, p. 12], we have the following result:

**Proposition 2.4.** *If $n \equiv 2 \pmod 4$, then $m^2+n-1 = q_1^2+q_2^2$ where $q_1$ and $q_2$ are integers.*

## 3. Constructions

In this section, we present two basic construction techniques for non-skew symmetric solutions to (1.1).

We let $J$ be the matrix of all ones.

**Theorem 3.1.** *Let $B$ be a $(1,-1)$-matrix of order $v$ satisfying*

$$B^{\mathrm{T}}B = BB^{\mathrm{T}} = dI+\mu J, \tag{3.1}$$

*where $d$ and $\mu$ are integers, and*

$$JB = BJ. \tag{3.2}$$

*Then*

$$C=\begin{bmatrix} tI-J & B \\ -B^{\mathrm{T}} & tI-J \end{bmatrix}$$

*where* $t=\frac{1}{2}(v+\mu)$, *is a solution to* (1.1) *with* $n=2v$ *and* $m=-1+\frac{1}{2}(v+\mu)$.

**Proof.** It is simple to verify that $C$ is orthogonal. □

We observe that if $v \geqslant 2$, then $C$ is non-skew.

**Construction 3.2.** Using $B=J$, with $d=0$ and $\mu=v$, we obtain solutions with $n=2v$ and $m=-1+\frac{1}{2}n$.

**Construction 3.3.** Using $B=J-2I$ with $d=4$ and $\mu=v-4$, we obtain solutions with $n=2v$ and $m=-3+\frac{1}{2}n$.

**Construction 3.4.** Let $A$ be the incidence matrix of a $(v,k,\lambda)$-SBIBD, and define $B=2A-J$. Then $BB^{\mathrm{T}}=4(k-\lambda)I+(4\lambda-4k+v)J$ and $BJ=JB=(2k-v)J$. Thus, we obtain solutions with $n=2v$ and $m=2\lambda+v-2k-1$.

There are many infinite families of SBIBD's. For example, the Hadamard designs with $(v,k,\lambda)=(4t-1,2t-1,t-1)$ give solutions with $n=8t-2$ and $m=2t-2$. The projective planes with $(v,k,\lambda)=(t^2+t+1,t+1,1)$ give solutions with $n=2(t^2+t+1)$ and $m=t^2-t$. See [3, 5] for lists of $(v,k,\lambda)$-SBIBD's.

The next construction uses orthogonal designs. An *orthogonal design of order r* and type $(u_1,u_2,\ldots,u_s)$, $(u_i \geqslant 0)$ on the commuting variables $x_1,x_2,\ldots,x_s$ is a matrix $D$ of order $r$ with entries $\{0,\pm x_1,\ldots,\pm x_s\}$ such that

$$DD^{\mathrm{T}}=\sum_{i=1}^{s}(u_i x_i^2)I.$$

The matrix $D$ can be written as $D=x_1A_1+\cdots+x_sA_s$ where $A_iA_i^{\mathrm{T}}=u_iI$. An orthogonal design is *full* if $r=\sum_{i=1}^{s}u_i$, or equivalently if 0 is not used. The usual definition of orthogonal designs requires that $u_i>0$. We have relaxed it and allowed some of the $u_i$'s to be 0 in order that some constructions can be presented in a systematic manner.

**Theorem 3.5.** *Suppose* $D=x_1I+x_2A_2+\cdots+x_sA_s$ *is a full orthogonal design of order r and type* $(1,u_2,\ldots,u_s)$ *and suppose that* $B_1,\ldots,B_s$ *are matrices of order v, such that*:

$$B_1 \text{ has } m\text{'s on the diagonal and } \pm 1 \text{ elsewhere}; \tag{3.3}$$

$$B_2,\ldots,B_s \text{ are } (+1,-1)\text{-matrices}; \tag{3.4}$$

$$B_iB_j^{\mathrm{T}}=B_jB_i^{\mathrm{T}} \quad \text{for all } i,j; \tag{3.5}$$

$$B_1B_1^{\mathrm{T}}+\sum_{i=2}^{s}\mu_iB_iB_i^{\mathrm{T}}=(m^2+rv-1)I. \tag{3.6}$$

*Then* $C=B_1\otimes I+\sum_{i=2}^{s}B_i\otimes A_i$ *is a solution to* (1.1).

**Proof.** This construction essentially replaces the variable $x_i$ of an orthogonal design by a matrix $B_i$. Conditions (3.3) and (3.4) ensure that the resulting matrix $C$ has $m$'s on the diagonal and $\pm 1$'s elsewhere. Condition (3.5) implies that the matrix multiplication commutes. Since $D$ is an orthogonal matrix, $CC^{\mathrm{T}}$ considered as block matrix multiplication has zeros on the off diagonal blocks. Condition (3.6) implies that the diagonal blocks have $m^2+rv-1$ on the diagonal and zeros elsewhere. □

In applying this theorem, we usually choose $B_1$ to be $(m+1)I-J$, $B_2$ to be $J$ and $B_3$ to be $J-2I$. In this case, the following weaker results suffices:

**Corollary 3.6.** *Suppose $D=x_1A_1+\cdots+x_sA_s$ is a full orthogonal design of order $r$ and type $(1, u_2, \ldots, u_s)$ and suppose that $B_2, \ldots, B_s$ are $(+1, -1)$-matrices of order $v$, such that*

$$B_i=B_i^{\mathrm{T}} \quad \textit{for } 2\leqslant i\leqslant s; \tag{3.7}$$

$$B_iJ=JB_i \quad \textit{for } 2\leqslant i\leqslant s; \tag{3.8}$$

$$B_iB_j=B_jB_i \quad \textit{for } 2\leqslant i, j\leqslant s; \tag{3.9}$$

$$\sum_{i=2}^{s} u_iB_i^2=dI+\mu J. \tag{3.10}$$

*Then $C=[(m+1)I-J]\otimes I+\sum_{i=2}^{s} B_i\otimes A_i$ is a solution to (1.1) with $n=vr$ and $m=-1+\frac{1}{2}(v+\mu)$.*

**Proof.** It is simple to show that conditions (3.7) to (3.10) together with the choice of $m$ imply the conditions (3.3) to (3.6). □

**Construction 3.7.** If a full orthogonal design of order $r$ and type $(1, u_2, u_3)$ exists, then a solution to (1.1) exists with $n=rv$ and $m=-1-2u_3+\frac{1}{2}n$, using $B_2=J$ and $B_3=J-2I$. Suppose, in particular, that $2^t$ divides $n$. Since every orthogonal design of order $2^t$ exists, it follows that a solution to (1.1) exists for $m=\frac{1}{2}n-1-2i$, $i=0, 1, \ldots, 2^t-1$.

**Construction 3.8.** If a $(v, k, \lambda)$-SBIBD with a symmetric incidence matrix $A$ exists and if there exists a full orthogonal design of orer $r$ and type $(1, u_2, u_3, u_4)$, then there exists a solution to (1.1) with $n=vr$ and $m=\frac{1}{2}n-1-2u_3-2(k-\lambda)u_4$, using $B_2=J$, $B_3=J-2I$ and $B_4=2A-J$. Here, we need a symmetric $A$ because of condition (3.7). Since $A$ has constant line sum $k$, $B_4$ has constant line sum $2k-v$ and (3.8) is satisfied.

One should mention that whenever there exists a $(v, k, \lambda)$-difference set over an abelian group, the incidence matrix can be made to be symmetrical [7, p. 280–293]. In particular, Theorem 6.1 of [4] is the special case of using quadratic residue difference sets.

Theorem 6.3 of [6] uses orthogonal designs of type $(1, u_2, u_3, u_4, u_5)$ with $u_4 = u_5$ and matrices $B_2 = J$, $B_3 = J - 2I$, $B_4 = Q + I$ and $B_5 = Q - I$ where $Q$ is the symmetric matrix obtained from quadratic residues modulo a prime power $v \equiv 1 \pmod 4$ [7, p. 291, Lemma 1.19].

## 4. Case $n \equiv 0 \pmod 4$, $m$ even

In this section, we prove the result that if $n \equiv 0 \pmod 4$ and $m > 1$ is even, then any solution to (1.1) must be skew-symmetric. We first establish some preliminary results.

Assume that a solution $C$ is non-skew. Then, without loss of generality, we can assume that the first three rows are of the form in Fig. 2.1 with $x_1 = x_2 = x_3 = 1$. Thus, (2.5) becomes

$$(3 + x_4 + x_5 + x_6)(m+1) + 4a = n. \tag{4.1}$$

**Lemma 4.1.** *If $C$ is a non-skew solution, $n \equiv 0 \pmod 4$ and $m$ is even, then $x_4 + x_5 + x_6$ is either equal to $-3$ or $1$.*

**Proof.** Equation (4.1) taken modulo 4 implies that $x_4 + x_5 + x_6 \equiv 1 \pmod 4$. Since the $x_i$'s are $\pm 1$'s, the sum must be either $-3$ or $1$. □

One should remark that the conclusion of Lemma 4.1 applies to any $3 \times 3$ principal submatrix of $C$, as long as $x_1 = x_2 = x_3 = 1$.

**Lemma 4.2.** *If $C$ is a non-skew solution, $n \equiv 0 \pmod 4$ and $m$ is even, then $m \leqslant \frac{1}{4}n - 1$.*

**Proof.** If $x_4 + x_5 + x_6 = 1$, then (4.1) implies that $4(m+1) + 4a = n$. Since $a \geqslant 0$, we have $m \leqslant \frac{1}{4}n - 1$.

If $x_4 + x_5 + x_6 = -3$, we multiply the whole of row 3 and column 3 by $-1$ and then take the transpose of $C$. We can normalise the new row 1 back to the required form. However, the new matrix has only $x_5 = -1$ and the analysis for the case $x_4 + x_5 + x_6 = 1$ now applies. □

We organize the non-skew solution $C$ as in Fig. 4.1.

$$C = \left[\begin{array}{cc|c|c} m & 1 & 1\cdots 1 & 1\cdots 1 \\ 1 & m & 1\cdots 1 & -\cdots- \\ \hline \multicolumn{2}{c|}{Y} & Z & * \\ \hline \multicolumn{2}{c|}{*} & * & * \end{array}\right] \begin{array}{l} \left.\begin{array}{c} \\ \\ \end{array}\right\} 2 \\ \left.\begin{array}{c} \\ \end{array}\right\} \tfrac{1}{2}n - 1 - m \\ \\ \end{array}$$

$$\underbrace{\qquad}_{2} \quad \underbrace{\qquad}_{\frac{1}{2}n-1-m}$$

Fig. 4.1.

It is easy to show that the number of columns beginning with $(1,1)^{\mathrm{T}}$ is $\frac{1}{2}n-1-m$ as shown in Fig. 4.1. Lemma 4.2 implies that $\frac{1}{2}n-1-m \geqslant \frac{1}{4}n$ and thus the matrixes $Y$ and $Z$ are non-vacuous. We choose to index the rows of $Y$ and the rows and columns of $Z$ from 3 to $\frac{1}{2}n+1-m$. The portions marked by $*$ are not of interest in the proof of our main result.

**Lemma 4.3.** *If $C$ is a non-skew solution organized as in Fig.* 4.1, $n \equiv 0 \pmod 4$ *and $m$ is even, then the rows of $Y$ are either* $(1,-1)$ *or* $(-1,1)$.

**Proof.** By appropriate row and column permutation, any row of $Y$ can be permuted to row 3 of $C$. Since $x_4 = 1$, Lemma 4.1 implies that $x_5$ and $x_6$ must have opposite sign. $\square$

We further organise the non-skew solution $C$ as in Fig. 4.2.

$$
\begin{array}{cl}
C = \left[\begin{array}{cc|c|c|c}
m \quad 1 & & 1\cdots 1 & 1\cdots 1 & 1\cdots 1 \\
1 \quad m & & 1\cdots 1 & 1\cdots 1 & -\cdots - \\
\hline
1 \;\vdots\; - & & & & \\
 & & W_1 & W_2 & * \\
1 \;\vdots\; - & & & & \\
\hline
- \;\vdots\; 1 & & & & \\
 & & W_3 & W_4 & * \\
- \;\vdots\; 1 & & & & \\
\hline
* & & * & * & *
\end{array}\right]
&
\begin{array}{l}
\left.\vphantom{\begin{array}{c}1\\1\end{array}}\right\} a \\
\left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} \alpha \\
\left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} \beta \\
\vphantom{*}
\end{array}
\\
\qquad\quad \underbrace{\qquad}_{2} \quad \underbrace{\qquad}_{\alpha} \quad \underbrace{\qquad}_{\beta} &
\end{array}
$$

Fig. 4.2.

In Fig. 4.2, $\alpha$ and $\beta$ are the number of rows of $Y$ of the form $(1,-1)$ and $(-1,1)$ respectively. The matrices $W_1$ to $W_4$ represent a further partitioning of $Z$. The indices for their rows and columns are the same as those for $C$.

**Lemma 4.4.** *If $C$ is a non-skew solution organised as Fig.* 4.2, $n \equiv 0 \pmod 4$ *and $m$ is even, then $W_1$ and $W_4$ are skew-symmetric and $W_2 = W_3^{\mathrm{T}}$.*

**Proof.** We shall prove the equivalent statement that $Z_{ij} = -Z_{ji}$ if row $i$ of $Y$ is the same as row $j$ of $Y$ and $Z_{ij} = Z_{ji}$ if row $i$ of $Y$ is the negative of row $j$ of $Y$.

If row $i$ and row $j$ of $Y$ are both $(1,-1)$, then the $3\times 3$ principal submatrix formed by rows 1, $i$ and $j$ and the corresponding columns is

$$
\begin{array}{llll}
\text{row } 1: & m & 1 & 1 \\
\text{row } i: & 1 & m & Z_{ij} \\
\text{row } j: & 1 & Z_{ji} & m.
\end{array}
$$

Lemma 4.1 implies that $Z_{ij} = -Z_{ji}$.

If row $i$ and row $j$ of $Y$ are both $(-1,1)$, then we take the $3\times 3$ principal submatrix formed by rows 2, $i$ and $j$. Again Lemma 4.1 implies that $Z_{ij} = -Z_{ji}$.

If row $i$ of $Y$ is $(1,-1)$ and row $j$ of $Y$ is $(-1,1)$, then the $3\times 3$ principal submatrix formed by rows 1, $i$ and $j$ is

| | | | |
|---|---|---|---|
| row 1: | $m$ | 1 | 1 |
| row $i$: | 1 | $m$ | $Z_{ij}$ |
| row $j$: | $-$ | $Z_{ji}$ | $m$. |

Lemma 4.1 implies that $Z_{ij}=Z_{ji}$.

The remaining case of row $i=(-1,1)$ requires a similar proof. □

**Theorem 4.5.** *If $n\equiv 0 \pmod 4$ and $m>1$ is even, then any solution $C$ to (1.1) is skew symmetric.*

**Proof.** Assume that $C$ is non-skew. Then it can be organised as in Fig. 4.2. We count and equate the number of $+1$'s in $W_2$ and $W_3$ to show that $m=0$.

The number of $+1$'s in $W_1$ is $\frac{1}{2}\alpha(\alpha-1)$. The number of $+1$'s in each row of $Z$ is $a=\frac{1}{4}n-1-m$ as given by (4.1) with $x_4+x_5+x_6=1$. Thus the number of $+1$'s in $W_2$ is $a\alpha-\frac{1}{2}\alpha(\alpha-1)$. Similarly, the number of $+1$'s in $W_3$ is $a\beta-\frac{1}{2}\beta(\beta-1)$. Since $W_2=W_3^{\mathrm{T}}$, we have

$$a\alpha-\tfrac{1}{2}\alpha(\alpha-1)=a\beta-\tfrac{1}{2}\beta(\beta-1),$$

which implies that

$$(\alpha-\beta)(2a+1)=(\alpha-\beta)(\alpha+\beta). \tag{4.2}$$

But $\alpha+\beta=\frac{1}{2}n-1-m$ is odd under the assumption of the Theorem. Therefore $\alpha\neq\beta$ and (4.2) implies that $2a+1=\alpha+\beta=\frac{1}{2}n-1-m$. Using $a=\frac{1}{4}n-1-m$, we have $2a+1=\frac{1}{2}n-1-2m$ which implies that $m=0$. □

One should note that when $m=0$, a result of Delsarte–Goethals–Seidel [2] states that every orthogonal matrix of order $s\equiv 0 \pmod 4$ can be switched into a skew-symmetric form by changing the signs of rows and columns. However, these sign changes need not apply simultaneously to rows and columns.

## 5. Case $n\equiv 2 \pmod 4$, $m\geqslant\frac{1}{6}n$

In this section, we study the case $n\equiv 2 \pmod 4$, $m$ even and $m\geqslant\frac{1}{6}n$. In particular, we analyse the structure of a non-skew solution $C$ and derive some necessary conditions.

**Proposition 5.1.** *Let*

$$Q=\begin{bmatrix} m & x_1 & x_2 \\ x_3 & m & x_4 \\ x_5 & x_6 & m \end{bmatrix}$$

*be any* $3\times 3$ *principal submatrix of a solution* $C$ *to* (1.1). *If* $n\equiv 2 \pmod 4$ *and* $m$ *is even, then* $x_1+x_2+\cdots+x_6\equiv 2 \pmod 4$.

**Proof.** We can permute $Q$ to be the principal submatrix of the first 3 rows and force these rows to be of the form in Fig. 2.1. Equation (2.5) taken modulo 4 implies $x_1x_6+x_2x_4+x_3x_5\equiv 3 \pmod 4$. One can then show that the number of $x_i$'s $=-1$ is even and then $x_1+\cdots+x_6\equiv 2 \pmod 4$. $\square$

**Proposition 5.2.** *If* $n\equiv 2 \pmod 4$, *m even and* $m\geq \frac{1}{6}n$, *then the following* $3\times 3$ *principal submatrices do not exist in a solution* $C$:

$$\begin{bmatrix} m & 1 & 1\\ 1 & m & 1\\ 1 & 1 & m\end{bmatrix},\quad \begin{bmatrix} m & - & -\\ - & m & 1\\ - & 1 & m\end{bmatrix},$$

$$\begin{bmatrix} m & 1 & -\\ 1 & m & -\\ - & - & m\end{bmatrix}\quad \text{and}\quad \begin{bmatrix} m & - & 1\\ - & m & -\\ 1 & - & m\end{bmatrix}.$$

**Proof.** In the first case, (2.5) implies that $6m+6+4a=n$. Since $a\geq 0$, we have $m\leq \frac{1}{6}n-1$, contradicting the assumption $m\geq\frac{1}{6}n$. The other three cases can all be reduced to the first case by changing the signs of one row and one column. $\square$

If $C$ is a non-skew solution, then we can force $C_{12}=C_{21}=1$, and the first row to be all 1's. Considering the first two rows of $C$, it is easy to show that it has $\frac{1}{2}n-1+m$ subcolumns of the form $(1,-1)$ and $\frac{1}{2}n-1-m$ subcolumns of the form $(1,1)$. Thus $C$ can be forced into the form of Fig. 5.1.

$$C=\left[\begin{array}{cc|c|c} m & 1 & 1\cdots 1 & 1\cdots 1\\ 1 & m & -\cdots - & 1\cdots 1\\ \hline \multicolumn{2}{c|}{Y_1} & * & *\\ \hline \multicolumn{2}{c|}{Y_2} & * & * \end{array}\right]$$

Fig. 5.1.

**Proposition 5.3.** *If* $n\equiv 2 \pmod 4$, *m even,* $m\geq\frac{1}{6}n$ *and* $C$ *is a non-skew solution as shown in Fig.* 5.1, *then the rows of* $Y_1$ *are either* $(1,-1)$ *or* $(-1,1)$ *and the rows of* $Y_2$ *are all* $(-1,-1)$.

**Proof.** The $3\times 3$ principal submatrix formed by rows 1, 2 and a row of $Y_1$ is

$$\begin{bmatrix} m & 1 & 1\\ 1 & m & -\\ x_5 & x_6 & m\end{bmatrix}.$$

Proposition 5.1 implies that $x_5=-x_6$ and hence the rows of $Y_1$ must be either $(1,-1)$ or $(-1,1)$. Similar arguments with the principal submatrix formed by rows

1, 2 and a row of $Y_2$ shows that the rows of $Y_2$ must be either (1, 1) or $(-1,-1)$. However, the case (1, 1) is impossible because it is forbidden by Proposition 5.2. □

Let $\alpha$ and $\beta$ be the number of rows in $Y_1$ of the form $(1,-1)$ and $(-1,1)$ respectively. We can now organise $C$ as in Fig. 5.2.

$$C=\left[\begin{array}{cc|c|c|c} m & 1 & 1\cdots1 & 1\cdots1 & 1\cdots1 \\ 1 & m & -\cdots- & -\cdots- & 1\cdots1 \\ \hline 1 & - & & & \\ \vdots & \vdots & W_1 & W_2 & W_3 \\ 1 & - & & & \\ \hline - & 1 & & & \\ \vdots & \vdots & W_4 & W_5 & W_6 \\ - & 1 & & & \\ \hline - & - & & & \\ \vdots & \vdots & W_7 & W_8 & W_9 \\ - & - & & & \end{array}\right]\begin{array}{l} \\ \\ \left.\begin{array}{l}\}\alpha\\ \\ \\ \}\beta\end{array}\right\}(\tfrac{1}{2}n-1-m) \\ \\ \}(\tfrac{1}{2}n-1-m) \end{array}$$

$$\qquad\qquad\qquad\qquad\quad \underbrace{\qquad}_{\alpha}\qquad\underbrace{\qquad}_{\beta}$$

Fig. 5.2.

The next few results show the structure of the submatrices $W_1$ to $W_9$.

**Proposition 5.4.** *If* $n \equiv 2 \pmod 4$, *m even,* $m \geq \frac{1}{6}n$ *and a non-skew solution C is organised as in Fig.* 5.2, *then*:

$$W_1 = (m+1)I - J; \tag{5.1}$$

$$W_2 = -W_4^{\mathrm{T}}; \tag{5.2}$$

$$W_3 = -W_7^{\mathrm{T}}; \tag{5.3}$$

$$W_6 = W_8^{\mathrm{T}}; \tag{5.4}$$

$W_5$ *and* $W_9$ *are symmetric matrices.* (5.5)

**Proof.** Throughout this proof, we let $z_1 = C_{ij}$ with $i \neq j$ and $z_2 = C_{ji}$. A $3\times3$ principal submatrix is formed using these two entries and an extra row and column chosen as the situation requires.

To prove (5.1), we take $z_1$ and $z_2$ from $W_1$ and use row 2 of $C$ to obtain the $3\times3$ matrix

$$\begin{bmatrix} m & - & - \\ - & m & z_1 \\ - & z_2 & m \end{bmatrix}.$$

Propositions 5.1 and 5.2 together imply that $z_1 = z_2 = -1$.

To prove (5.2), we take $z_1$ from $W_2$, $z_2$ from $W_4$ and use row 2 to form submatrix. Proposition 5.1 implies that $z_1 = -z_2$.

The rest of the proof is similar. □

**Proposition 5.5.** *If $n \equiv 2 \pmod 4$, $m$ even, $m \geq \frac{1}{6}n$ and a non-skew solution $C$ is organised as in Fig. 5.2, then:*

$$\textit{each of } W_7 \textit{ and } W_8 \textit{ has constant column sum } 0; \tag{5.6}$$

$$W_9 \textit{ has constant column sum } m+1; \tag{5.7}$$

$$W_4 \textit{ has constant column sum } 2m-\alpha. \tag{5.8}$$

**Proof.** We use the fact that the columns of $C$ are orthogonal. We then study the inner product of an arbitrary column with columns 1 and 2.

For $W_7$ we take an arbitrary column $i$ where $3 \leq i \leq \alpha+2$. We let $r_1$, $s_1$ and $t_1$ be the number of $+1$'s in a column of $W_1$, $W_4$ and $W_7$ respectively. Similarly, $r_2$, $s_2$ and $t_2$ are the number of $-1$'s in a column of $W_1$, $W_4$ and $W_7$. The inner product of column $i$ with columns 1 and 2 imply

$$2m-1+(r_1-r_2)-(s_1-s_2)-(t_1-t_2)=0, \tag{5.9}$$

and

$$-2m+1-(r_1-r_2)+(s_1-s_2)-(t_1-t_2)=0. \tag{5.10}$$

Adding (5.9) and (5.10), we get $t_1-t_2=0$, which is also the column sum of $W_7$. Similarly, one can show that the column sums of $W_8$ and $W_9$ are 0 and $m+1$ respectively.

Furthermore, (5.1) implies that $r_1=0$ and $r_2=\alpha-1$. Thus, (5.10)–(5.9) implies that $s_1-s_2=2m-\alpha$ which proves (5.8). □

We will show that the number of $-1$'s in each row of $W_5$ is the same. We let this number be $\gamma-1$. The next result gives the structure of the remaining symmetric portion of $C$.

**Proposition 5.7.** *If $n \equiv 2 \pmod 4$, $m$ even, $m \geq \frac{1}{6}n$ and a non-skew solution $C$ is organised as in Fig. 5.2, then the submatrix formed by $W_5$, $W_6$, $W_8$ and $W_9$ can be permuted into the form of Fig. 5.3, where $J$ is a matrix of all 1's.*

$$\begin{array}{c}
\left[\begin{array}{c|c|c|c}
\begin{smallmatrix} m & & - \\ & \ddots & \\ - & & m \end{smallmatrix} & J & J & -J \\ \hline
J & \begin{smallmatrix} m & & - \\ & \ddots & \\ - & & m \end{smallmatrix} & -J & J \\ \hline
J & -J & \begin{smallmatrix} m & & - \\ & \ddots & \\ - & & m \end{smallmatrix} & J \\ \hline
-J & J & J & \begin{smallmatrix} m & & - \\ & \ddots & \\ - & & m \end{smallmatrix}
\end{array}\right]
\begin{array}{l}
\left.\right\}\gamma \quad \left.\right\}\beta \\
\\
\left.\right\}\tfrac{1}{2}(\tfrac{1}{2}n-1-m) \\
\left.\right\}\tfrac{1}{2}(\tfrac{1}{2}n-1-m)
\end{array} \\
\underbrace{\underbrace{\quad}_{\gamma}\quad}_{\beta} \qquad \underbrace{\qquad\qquad}_{\text{each is } \frac{1}{2}(\frac{1}{2}n-1-m)}
\end{array}$$

Fig. 5.3.

**Proof.** Suppose the first row of $W_5$ has $(\gamma-1)$ $-1$'s. Permute the columns (and rows) such that this first row is $(m - \cdots - 1 \cdots 1)$. Partition $W_5$ into

$$\begin{bmatrix} G_1 & G_2 \\ G_3 & G_4 \end{bmatrix}$$

where $G_1$ and $G_4$ are square submatrices of order $\gamma$ and $\beta-\gamma$ respectively.

Any principal submatrix of $G_1$ containing the first row is of the form

$$\begin{bmatrix} m & - & - \\ - & m & z \\ - & z & m \end{bmatrix}.$$

Proposition 5.2 implies that $z=-1$. Thus $G_1$ is $(m+1)I-J$.

By considering a principal submatrix containing the first row as well as an entry from $G_2$ (not from row 1) and the corresponding entry in $G_3$, we obtain $G_2=J=G_3^{\mathrm{T}}$. Similarly, we can show that $G_4=(m+1)I-J$

The proof that $W_9$ is partitioned as shown in Fig. 5.3 follows a similar proof, except that the two blocks of $(m+1)I-J$ are of equal size $\frac{1}{2}(\frac{1}{2}n-1-m)$.

The partition of $W_5$ and $W_9$ implies a partitioning of $W_6$ into

$$\underbrace{\left[\begin{array}{c|c} H_1 & H_2 \\ \hline H_3 & H_4 \end{array}\right]}_{\substack{\text{each is} \\ \frac{1}{2}(\frac{1}{2}n-1-m)}} \begin{array}{l} \}\gamma \\ \phantom{x} \end{array}\Big\}\beta$$

Using similar arguments, we can show that $H_1$ is either $J$ or $-J$ and that $H_2=-H_1$. Thus, by permitting the two column blocks, if necessary, we can assume $H_1=J$ and $H_2=-J$. Now, it is simple to find the structures of $H_3$, $H_4$ and $W_8$.

One should mention that the degenerate cases $\gamma=0$, $\beta-\gamma=0$ or $(\frac{1}{2}-1-m)\leqslant 2$ are either trivial or can be easily taken care of. $\square$

Hence, in the case of $n\equiv 2 \pmod 4$, $m$ even and $m\geqslant\frac{1}{6}n$, a non-skew solution is completely determined by the variables $\alpha$, $\beta$, $\gamma$ and the matrices $W_4$ and $W_7$. By block permutations, we can assume that $\gamma\geqslant\beta-\gamma$. Next, we count the number of $+1$'s and $-1$'s in $W_4$ and $W_7$ in order to derive further necessary conditions involving $\alpha$, $\beta$ and $\gamma$.

**Proposition 5.8.** *If $n\equiv 2 \pmod 4$, $m$ even, $m\geqslant\frac{1}{6}n$ and a non-skew solution $C$ is organised as shown in Figs. 5.2 and 5.3, then:*

*the number of $+1$'s in each column of $W_4$ is $m-\frac{1}{2}(\alpha-\beta)$;* (5.11)

*the number of $+1$'s in each column of $W_7$ is $\frac{1}{2}(\frac{1}{2}n-1-m)$;* (5.12)

*the number of $+1$'s in each row of $W_4$ is*

*$\frac{1}{2}(\frac{1}{2}n-1+m)-1-(\beta-\gamma)$ for the first $\gamma$ rows and*

*$\frac{1}{2}(\frac{1}{2}n-1+m)-1-\gamma$ for the remaining $\beta-\gamma$ rows;* (5.13)

*the number of* $+1$*'s in each row of* $W_7$ *is*

$\frac{1}{2}(\frac{1}{2}n-1+m)-\gamma$ *for the first* $\frac{1}{2}(\frac{1}{2}n-1-m)$ *rows and*

$\frac{1}{2}(\frac{1}{2}n-1+m)-(\beta-\gamma)$ *for the remaining* $\frac{1}{2}(\frac{1}{2}n-1-m)$ *rows.* (5.14)

**Proof.** Conditions (5.11) and (5.12) follow easily from (5.8) and (5.6).

Equation (2.7), applied to the first and second rows of $C$ as well as a row with a section in $W_4$, gives the number of $+1$'s in a row of $W_4$ and $W_5$. Since $W_5$ is known, the number of $+1$'s in a row of $W_4$ can be computed as shown in (5.13). Condition (5.14) is similar. □

**Proposition 5.9.** *If* $n \equiv 2 \pmod 4$, $m$ *even,* $m \geq \frac{1}{6}n$ *and a non-skew solution* $C$ *is organised as shown in Figs.* 5.2 *and* 5.3, *then the following conditions hold*:

$$\alpha[m-\tfrac{1}{2}(\alpha-\beta)]=\tfrac{1}{2}\beta(\tfrac{1}{2}n-1+m)-\beta-2\gamma(\beta-\gamma); \tag{5.15}$$

$$(\beta-2\gamma)^2(\tfrac{1}{2}n-1-m)+\gamma(2\gamma-\beta-2)^2+(\beta-\gamma)(\beta-2\gamma-2)^2 \\ =\alpha[(\alpha-1)(2m-\alpha)+\tfrac{1}{2}n-1-m+\beta]; \tag{5.16}$$

$$\textit{if } \tfrac{1}{2}n>m+3 \textit{ or } \gamma\geq 2, \textit{ then } \alpha\geq|\tfrac{1}{2}n-1-3m+\beta|; \tag{5.17}$$

$$\textit{if } \tfrac{1}{2}n-1-m\geq 6 \textit{ or } \gamma\geq 3, \textit{ then } \alpha\geq 3[\tfrac{1}{2}n-1-3m+\beta]. \tag{5.18}$$

**Proof.** Condition (5.15) follows by counting the number of $+1$'s in $W_4$ first by columns and then by rows.

If $\frac{1}{2}n>m+3$, then the bottom row block of Fig. 5.3 has at least 2 rows. Consider the inner product of the bottom 2 rows. Without considering the contribution from $W_7$, the inner product is $\frac{1}{2}n-1-3m+\beta$. The inner product of 2 rows of $W_7$ is at most $\pm\alpha$. The total inner product is 0 which implies (5.17), If $\gamma\geq 2$, then we take the inner product of 2 rows of $C$ containing the top 2 rows of Fig. 5.3.

Under the assumption of (5.18), either the bottom or top row blocks of Fig. 5.3 contain at least 3 rows. Thus, there exists a $3\times\alpha$ submatrix $X$ of either $W_4$ or $W_7$ where the inner product of two distinct rows is $-[\frac{1}{2}n-1-3m+\beta]$. The row inner product of $X$ is not changed by changing signs of whole columns. Thus we make the first row of $X$ all $+1$'s. We let $z_1$, $z_2$, $z_3$ and $z_4$ be the number of columns of $X$ of the form $(1,1,1)^T$, $(1,1,-1)^T$, $(1,-1,1)^T$ and $(1,-1,-1)^T$. We write down the 4 equations obtained by considering inner products and number of columns.

$$z_1+z_2+z_3+z_4=\alpha,$$
$$z_1-z_2+z_3-z_4=-[\tfrac{1}{2}n-1-3m+\beta],$$
$$z_1+z_2-z_3-z_4=-[\tfrac{1}{2}n-1-3m+\beta],$$
$$z_1-z_2-z_3+z_4=-[\tfrac{1}{2}n-1-3m+\beta].$$

Adding the equations, we get

$$4z_1=\alpha-3[\tfrac{1}{2}n-1-3m+\beta].$$

Since $z_1\geq 0$, (5.18) follows.

To prove (5.16), we consider the sumatrix $X$ formed by $W_2$ and $W_3$. The product $XX^T$ has $\frac{1}{2}n-1-m+\beta$ on the diagonal and $2m-\alpha$ elsewhere. Condition (5.16) is obtained by considering $JXX^TJ$. □

For example, in the case $n=22$ and $m=4$, only 3 cases of $(\alpha,\beta,\gamma)$ satisfies (5.15), namely, (2, 12, 9), (4, 10, 8) and (9, 5, 3). The first two cases are eliminated by (5.17). The last case exists by using the (11, 5, 2)-SBIBD and Construction 3.4. The case $(n,m,\alpha,\beta,\gamma)=(10,2,4,2,2)$ satisfies (5.15) and neither (5.17) nor (5.18) applies. But it is eliminated by (5.16). It is worth noting that in all cases with $n\leqslant 50$ where Proposition 5.9 applies, either the parameter $(n,m)$ is ruled out or there is a unique set of $(\alpha,\beta,\gamma)$ satisfying the conditions (5.15) to (5.18) and the solution exists. One wonders if this phenomenon is true in general.

## 6. Unsolved cases

In this section, we give a list of parameters with $n\leqslant 50$ and $m>1$ for which the existence of a non-skew solution is unknown. (See Table 1) There are 95 parameter sets within this range for which non-skew solutions are constructed.

Table 1
List of unsolved cases.

| $n$ | $m$ | $n$ | $m$ |
|---|---|---|---|
| 22 | 2 | 42 | 4 |
| 26 | 2 | 42 | 6 |
| 30 | 4 | 44 | 5 |
| 34 | 2 | 46 | 2 |
| 34 | 4 | 46 | 4 |
| 36 | 9 | 46 | 6 |
| 38 | 2 | 50 | 2 |
| 38 | 4 | 50 | 4 |
| 42 | 2 | 50 | 8 |

## References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, Vol. 182 (Springer-Verlag, Berlin, 1971).

[2] P. Delsarte, J.M. Goethals and J.J. Seidel, Orthogonal matrices with zero diagonal II, Canad. J. Math. 23 (1971) 816–832.

[3] J.W. Di Paola, J.S. Wallis and W.D. Wallis, A List of $(v,b,r,k,\lambda)$ designs for $r\leqslant 30$, Proc. 4th S.E. Conf. on Combinatorics, Graph Theory and Computing (1973) 249–258.

[4] A.V. Geramita and J. Seberry, Orthogonal designs, quadratic forms and Hadamard matrices, Lecture Notes in Pure and Applied Mathematics, Vol. 45 (Marcel Dekker, New York, 1979).

[5] M. Hall, Jr., Combinatorial Theory (Blaisdell, Waltham, MA, 1967).

[6] J. Seberry and C. Lam, On orthogonal matrices with constant diagonals, Linear Algebra Appl. 46 (1982) 117–129.

[7] W.D. Wallis, A.P. Street and J.S. Wallis, Combinatorics: Room Squares, Sum-Free Sets and Hadamard Matrices, Lecture Notes in Mathematics, Vol. 292 (Springer-Verlag, Berlin, 1972).